IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI ST. JOSEPH DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. 325,253.73 USDT SEIZED FROM TWO TETHER ADDRESSES Defendant.	Civil No.

COMPLAINT FOR FORFEITURE IN REM

Plaintiff, United States of America, by its attorneys, Jeffrey P. Ray, Acting United States Attorney for the Western District of Missouri, and John Constance, Assistant United States Attorney, brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

NATURE OF THE ACTION

1. This is an action to forfeit property to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C) based on violations of 18 U.S.C. §§ 1956 and 1343.

THE DEFENDANT IN REM

2. The defendant property consists of 325,253.73 Tether (USDT) stablecoin (the "Defendant Property") seized on or about December 16, 2024, from the following addresses stored at premises controlled by Tether Limited (the "Defendant Addresses"):

- **Defendant Address 1: 0xa761f652044774de9456316d008c57a41c8c5e7d**
- **Defendant Address 2: 0x9cfb73f0c8b494aaf8f00da25cd32286cf56ac98**

Tether Limited completed the transfer of the contents of the Defendant Addresses to the FBI on or about March 12, 2025. The Defendant Property is presently in the custody of the Federal Bureau of Investigation (FBI), Kansas City, Field Office.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a). This Court also has jurisdiction over this particular action under 18 U.S.C. § 981(a).

4. This Court has *in rem* jurisdiction over the defendant property pursuant to 28 U.S.C. § 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred in this district; and pursuant to 28 U.S.C. § 1355(b)(1)(B), incorporating 28 U.S.C. § 1395, because the Defendant Property was brought into this district following seizure outside of the United States.

5. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred in this district; and pursuant to 28 U.S.C. § 1395, because the Defendant Property was brought into this district following seizure outside of the United States.

BASIS FOR FORFEITURE

6. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C), because it constitutes, is derived from, or is traceable to proceeds of wire fraud, a "specified unlawful activity," as that term is defined in 18 U.S.C. § 1956(c)(7). The Defendant Property also is subject to forfeiture pursuant to

18 U.S.C. § 981(a)(1)(A) as property involved in money laundering, in violation of 18 U.S.C. § 1956.

FACTUAL ALLEGATIONS

I. Victim losses to Triangular currency investment scam

a. Victim #1

7. On or about April 17, 2024, an unidentified LinkedIn account holder who identified themselves with a fictitious name of Bertha Wright contacted Victim #1 through his/her LinkedIn account. Victim #1 resides in the Western District of Missouri. Wright claimed to live in Miami, Florida, been born in 1989, and work as a partner at a semiconductor company. Victim #1 communicated with Wright for a few days via LinkedIn before transitioning to WhatsApp. The conversations turned romantic, and Wright and Victim #1 continued to engage in text message conversations and sent multiple photographs of each other over the next approximately six weeks. The photographs of Wright sent to Victim #1 appear to have been generated by artificial intelligence.

8. On or about June 23, 2024, Wright introduced Victim #1 to a fictious cryptocurrency application called "Triangular." Wright explained to Victim #1 that Triangular was an extremely profitable cryptocurrency investment platform and sent Victim #1 a step-by-step guide to using the application.

9. Because Triangular is a fictitious platform, its operators can manipulate the value of the victim's account balance to show what appears to victims to be significant gains in the value of their investments. In reality, the victims' funds have

not been invested but rather moved from the deposit wallet address, through various intermediary wallets and, ultimately, cashed out by the illicit actors into alternative cryptocurrencies or fiat currency.

10. Between June 28, 2024, and August 7, 2024, Victim #1 transferred approximately $16 million in ETC and Bitcoin (BTC) to two Triangular wallets. Shortly after the initial deposit on June 28, 2024, it appeared to Victim #1 that his/her investment was growing exponentially, which encouraged him/her to continue depositing cryptocurrency into Triangular. Victim #1 sold stocks, various other investments, and used an inheritance to finance his/her transfers to Triangular.

11. After being contacted by the FBI in September 2024, Victim #1 realized they had been defrauded. Victim #1 then attempted to withdraw funds from his/her Triangular account, but all attempts were denied. Victim #1 contacted Triangular customer support to inquire about withdrawing funds and was told he/she could not withdraw funds until he/she had repaid a loan that he/she took against his/her earned interest to open a second Triangular account. According to the terms of the loan, Victim #1's funds would be confiscated if the loan was not repaid within a certain period of time.

b. Victim #2

12. In May 2024, Victim #2 received a direct message on LinkedIn from an account holder who identified themselves with a fictitious name of Elizabeth Jacques. Jacques initially reached out to Victim #2 in a professional capacity and shortly thereafter transitioned to communicating with Victim #2 via the same WhatsApp

number used to communicate with Victim #1. Sometime around June 2024, Jacques introduced Victim #2 to a cryptocurrency investment platform called DCG Triangle.

13. Victim#2 transferred approximately $70,000 dollars from his/her personal savings account to DCG Triangle. After only approximately two months, the Triangular application showed that Victim #2's investment had grown from $70,000 to approximately $1,000,000. Victim #2 attempted to withdraw money from Triangular but was blocked from doing so by the application. Victim #2 messaged customer service at dcgtriangle.com, but instead of providing support, DCG Triangle threatened to report Victim #2 to the FBI and other regulatory agencies for failing to pay Triangle's fees.

c. Victim #3

14. On September 3, 2024, a transfer of 1.4 Ether (ETH) cryptocurrency (~$3500) was made from a Kraken cryptocurrency exchange account to an address ending in -4679. The ETH was sent to another address ending in -3a4d then converted to USDT and subsequently transferred to Defendant Address #2.

15. Kraken identified the accountholder as M.M. ("Victim #3"). Victim #3 reported to FBI that he/she was contacted on LinkedIn by an individual who identified herself as Carolina Viktrova. Victim #3 and Viktrova initially discussed a business partnership. The discussion moved from LinkedIn to WhatsApp. Shortly after shifting the conversation to WhatsApp, Viktrova suggested to Victim #3 that he/she consider investing in cryptocurrency. Victim #3 agreed and "invested"

thousands of dollars in cryptocurrency over the ensuing months through investment scams suggested by Viktrova.

II. Tracing Victim funds through Defendant Addresses

16. Between June 28, 2024, and August 7, 2024, Victim #1 transferred approximately $16 million in ETH to a Triangular wallet address ending in -e9F3. Victim #1 also transferred USDT to the address.

17. These funds were rapidly disbursed by the criminal actor(s) across a vast web of additional wallets, including into Defendant Addresses #1 and #2.

18. On August 19, 2024, Defendant Address #1 directly received approximately $3,500 worth of ETH and USDT from the address ending in -e9F3. The deposit of ETH is the first transaction recorded on the blockchain ledger for Defendant Address #1.

19. Approximately two hours later, 300,000 USDT was sent to Defendant Address #1 from the address ending in -e9F3 in fourth-tier transactions. Of this 300,000 USDT, at least 195,000 USDT is directly traceable to Victim #1.

20. On July 25, 2024, Defendant Address #2 received 1,000,000 USDT directly from the Triangular address ending in -e9F3.

21. Between July 10 and August 14, 2024, an additional 1,900,000 USDT was sent from the Triangular wallet to Defendant Address #2 in two and three-tier transactions.

22. On September 3, 2024, in a two-tier transaction, Victim #3 transferred 1.4 ETH (~$3500) from his/her Kraken cryptocurrency exchange account to an

address ending in -e3a4d, which he/she believed was an investment account. The ETH was instead converted by the criminal actor(s) to USDT and subsequently sent directly to Defendant Address #2.

III. Use of Defendant Addresses to facilitate money laundering

23. The Defendant Addresses are being used to conceal and launder illicit funds; specifically, criminal proceeds from an international cryptocurrency scam in which subjects fraudulently induced victims to buy and transfer cryptocurrency through illegitimate investment businesses.

24. Between August 19, 2024, and October 18, 2024, Defendant Address #1 received approximately $1,860,000 in ETH, USDT, and USDC across 59 transactions from 11 different addresses. During that same period, Defendant Address #1 transferred approximately $1,860,000 in ETH, USDT, and USDC across 116 transactions to 18 different addresses.

25. A blockchain analysis of many of the addresses transacting with Defendant Address #1 show similar patterns of rapid, large-scale movement of cryptocurrency.

26. Between July 10, 2024, and October 16, 2024, Defendant Address #2 received approximately $12,670,000 in ETH and USDT across 201 transactions from 29 different addresses. During that same period, Defendant Address #2 transferred approximately $12,325,000 in ETH and USDT across 504 transactions to 42 different addresses.

27. The blockchain transactions of Defendant Addresses #1 and #2 are consistent with efforts to conceal the nature and source of the virtual currency, including a) rapid, large-scale and irregular movement of the tokens through multiple intermediary wallets with no apparent business purpose, b) transactions involving newly created or previously dormant addresses, and c) conversion into USDT from alternative virtual currencies for no apparent business purpose.

CLAIM FOR RELIEF

FIRST CLAIM FOR RELIEF

28. The Plaintiff repeats and incorporates by reference the paragraphs above.

29. By the foregoing and other acts, the Defendant Property, constitutes, or was derived from, proceeds traceable to specified unlawful activity, and therefore, is forfeitable to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C).

SECOND CLAIM FOR RELIEF

30. The Plaintiff repeats and incorporates by reference paragraphs 1 through 27 above.

31. By the foregoing and other acts, the Defendant Property constitutes property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or is traceable to such property, and therefore, is forfeitable to the United States, pursuant to 18 U.S.C. § 981(a)(1)(A).

WHEREFORE the United States prays that the defendant property be forfeited to the United States, that the plaintiff be awarded its costs and

disbursements in this action, and for such other and further relief as the Court deems proper and just.

Respectfully submitted,

JEFFREY P. RAY
Acting United States Attorney

By: */s/ John Constance*

John Constance
Assistant United States Attorney
400 E. 9th Street, Fifth Floor
Kansas City, Missouri 64106
Telephone: (816) 426-3122
E-mail: John.Constance@usdoj.gov

VERIFICATION

I, Special Agent **Savannah Latta**, hereby verify and declare under penalty of perjury that I am a Special Agent with the United States Federal Bureau of Investigation, that I have read the foregoing Verified Complaint in Rem and know the contents thereof, and that the factual matters contained in paragraphs 7 through 27 of the Verified Complaint are true to my own knowledge, except that those matters herein stated to be alleged on information and belief and as to those matters I believe them to be true.

The sources of my knowledge and information and the grounds of my belief are the official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Agent of the Federal Bureau of Investigation.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Dated 07/22/25

/s/ Savannah Latta
Savannah Latta
Special Agent
Federal Bureau of Investigation